

UNITED STATES DISTRICT COURT

for the
Eastern District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)THE PREMISES LOCATED AT 370 HOLLAND LANE,
UNIT 3013, ALEXANDRIA, VA, 22314, MORE
PARTICULARLY DESCRIBED IN ATTACHMENT ACase No. 1:17-SW- (UNDER SEAL)
274

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
31 USC 5314, 5322
22 USC 618
26 USC 7206(a)

Offense Description
Failure to file Foreign Bank Account Reports
Violation of Foreign Agent Registration Act
Filing a False Tax Return

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

[Redacted]

[Redacted Signature]

Special Agent, FBI

Printed name and title

/s/

Sworn to before me and signed in my presence.

Date: 5/27/2017City and state: Alexandria, VA

Theresa Carroli Buchanan
United States Magistrate Judge

Judge's signature

Hon. Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

MAY 27 2017

IN THE MATTER OF THE SEARCH)
OF THE STORAGE UNIT LOCATED AT)
370 HOLLAND LANE, UNIT 3013,)
ALEXANDRIA, VA, 22314,)
MORE PARTICULARLY DESCRIBED)
IN ATTACHMENT A)

Case No. 1:17-SW- 294

(Under Seal)

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, [REDACTED] being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to search the storage unit located at 370 Holland Lane, Unit 3013, Alexandria, Virginia 22314, which is described more particularly in Attachment A, in order to locate and seize the items described in Attachment B. Both Attachment A and Attachment B are incorporated by reference as though fully set forth in this affidavit.

2. I have been a Special Agent with the FBI since 2002. I have received basic law enforcement training at the FBI Academy in Quantico, Virginia. I am currently assigned to the FBI's International Corruption Squad in Washington, DC, where I am responsible for conducting and assisting in investigations relating to international corruption, money laundering, violations of the Foreign Corrupt Practices Act, and other related financial crimes.

3. The facts in this affidavit come from my personal observations, my training and experience, a review of documentary evidence, information provided by witnesses, and information obtained from other law enforcement agents. This affidavit is intended to show

merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe that violations of 31 U.S.C. §§ 5314, 5322(a) (Failure to File a Report of Foreign Bank and Financial Accounts), 22 U.S.C. § 618 (Foreign Agent Registration Act), and 26 U.S.C. § 7206(a) (Filing a False Tax Return), have been committed, and that there is probable cause to search the premises described in Attachment A for evidence, instrumentalities, contraband, or fruits of the crimes further described in Attachment B.

5. Since 2014, law enforcement agents have been conducting an investigation into, among other things, the financial dealings of Paul J. Manafort and Richard W. Gates. Manafort, a U.S. citizen, is and has been employed for many years as a lobbyist and political consultant working both in the United States and internationally. During all relevant times, he has been married to [REDACTED] with whom Manafort shares a joint interest in several bank accounts in the United States. Gates is also a U.S. citizen who is and has been employed as a lobbyist and political consultant working in the United States and internationally. During the relevant period, Gates worked as an employee of Manafort's.

6. Between 2005 and at least 2014, Manafort and Gates provided consulting services to former Ukrainian President Viktor Yanukovich, the Ukrainian political group the Party of Regions, and others. Manafort also performed work for other Ukrainians, to include Rinat Akhmetov, a former financial supporter of President Yanukovich, and Russian businessman Oleg Deripaska. During much of this time period, Manafort had a personal residence in Mount Vernon, Virginia, and a business office at [REDACTED] in Alexandria, Virginia.

7. Bank records show that, during this period, payments to Manafort's and Gates's domestic corporate and personal accounts came from numerous bank accounts in Cyprus, Latvia and Grenadines. The entries in the bank records indicate that many of these payments come from what appear to be foreign corporations. Information gathered by investigators, including the review of open source databases, reveals that Manafort controlled and/or held executive positions at the following domestic entities (which received funds from foreign financial accounts situated in Cyprus, Latvia, and Grenadines): Davis Manafort Partners, Inc. ("DMP Inc."), Davis Manafort, Inc., and DMP International LLC, Jesand Investment Corporation, and MC Soho Holdings, Inc. Domestic bank records reflect that Gates, Manafort's former associate, held signature authority over accounts in the name of Smythson LLC and DMP International, which also received funds from foreign financial accounts. Manafort and Gates held co-signature authority over domestic bank accounts in the names of DMP International LLC and DMP International.

8. A review of bank records shows that, during the following date ranges, funds were transferred from the following foreign companies' Cypriot, Latvian, or Grenadine bank accounts into Manafort's domestic accounts:

Foreign Sender	Dates	Domestic Beneficiary ¹	Amount
Antes Management	May 2006 – February 2007	Davis Manafort, Inc. Manafort and [REDACTED] [REDACTED] (hereinafter PJM/KBM)	\$4,225,364.33

¹ With the exception of Smythson LLC, Manafort held signatory authority and/or ownership interest on each of the domestic financial accounts receiving money from foreign sources. As discussed above, bank records reflect Manafort associate Gates as having signature authority on a domestic account in the name of Smythson LLC. Records for the Smythson LLC account reflect its receipt of funds from foreign senders identified in the table.

Foreign Sender	Dates	Domestic Beneficiary ¹	Amount
Yiakora Ventures	June 2008 – March 2011	Jessand PKM/KBM Davis Manafort, Inc. Davis Manafort Partners	\$15,151,000.00
Global Highway, Ltd	November 2009 – February 2012	Davis Manafort, Inc. PJM/KBM DMP International Davis Manafort Partners	\$7,917,500.00
Leviathan Advisors	June 2010 – December 2011	Davis Manafort, Inc. PJM/KBM Davis Manafort Partners	\$5,472,300.00
Peranova Holdings ²	November 2011 – February 2012	PJM/KBM DMP International	\$1,625,000.00
Bletilla Ventures	March 2012 – March 2013	DMP International Smythson LLC	\$5,730,000.00
Lucicle Consultants	March 2012 – May 2013	DMP International Smythson LLC PJM/KBM	\$2,864,348.06
Global Endeavor	September 2013 – October 2014	DMP International	\$1,744,869.67
Telmar Investments	January 2014 – June 2014	DMP International	\$2,750,000.00
TOTAL			\$47,480,381.73

9. In July 2014, Manafort and Gates were interviewed by the FBI. During those interviews, among other statements, Manafort and Gates acknowledged that they performed

² Money wired from Peranova Holdings on February 1, 2012, was used almost immediately to purchase real estate on Manafort's behalf. On February 9, 2012, \$1.5 million was transferred from DMP Inc., to the Manaforts' personal bank account at First Republic Bank. The next day it was transferred to the account of MC Soho Holding, LLC, which Manafort created the same day. Several days later, on February 14, 2012, the funds were used to purchase a \$2.85 million condominium at [REDACTED] in the SoHo neighborhood of Manhattan.

work on behalf of the Party of Regions and were paid for that work through foreign bank accounts. Although Manafort identified his formal client as the Party of Regions, during the interview he also described work he did on behalf of Yanukovych, Deripaska, and Akhmetov. During his interview with law enforcement, among other things, Gates said he was directed by Ukrainians to open accounts in Cyprus and Grenadines. Gates was told that it was easier for the Ukrainians to pay Gates and Manafort from one Cypriot account to another Cypriot account. Gates was also told that Ukrainians did not want others to know the identity of their campaign manager. Gates did not identify who told him how to coordinate the receipt of payment from Ukrainian clients. Gates did not specify how Cypriot and Grenadine accounts were opened, or by whom.

10. During his interview with law enforcement, Manafort stated that he was not a signatory on Cypriot bank accounts and was unsure who created the accounts, but acknowledged that he knew several companies were established in Cyprus in order for him to receive payment from the Ukrainians. Regarding these accounts and the manner of payment, Manafort stated that he had directed Gates and another employee to do what the Ukrainians wanted. Although Gates told law enforcement that the Ukrainians wanted to hide Manafort's identity, Manafort told agents that concealment was not necessary when these companies were established because he was providing political services in the public eye.

11. In addition to the nearly \$47 million wired directly into Manafort's domestic accounts, the FBI investigation has revealed that funds totaling more than \$6 million were wired directly from Cyprus and/or Grenadines foreign financial accounts to merchants, vendors, and investment accounts in the United States that appear to be expenditures made for the Manaforts' personal benefit because the vendors appear to be located close to the Manaforts' residences.

For example: in 2010, Global Highway wired \$250,000.00 to an Oriental Rug company located in Alexandria, Virginia and \$325,000.00 to men's clothing stores in New York City and Beverly Hills, California; from 2010-11, Leviathan Advisors wired \$240,000.00 to a landscaping company in Southampton, New York and \$49,425.00 to a company that provides vacation rentals in Italy; from 2011-13, Lucicle wired \$370,000.00 to a construction company in Palm Beach Gardens, Florida; \$80,000.00 to a landscaping company in Southampton, New York and \$1.9 million to a law firm in Virginia; in 2011, Global Endeavor wired \$200,000.00 to a horse farm in Wellington, Florida and in November, 2013, Global Endeavor sent wire transfers totaling \$29,000.00 to landscaping companies in New York and Florida. Thus far law enforcement agents have confirmed, through interviews with vendors, that payments directly from overseas accounts to the Oriental rug company, to the landscaping company in Southampton, to the men's clothing store in Los Angeles, and to the construction company in Palm Beach Gardens were for Manafort's benefit. Law enforcement agents continue to attempt to interview the other vendors. Based on my training and experience, these payments for Manafort's benefit indicate that Manafort likely held a financial interest in or control over those foreign financial accounts in order to have directly or indirectly caused such payments to be made from those foreign financial accounts to so many different recipients, .

12. The Department of the Treasury generally requires U.S. citizens and U.S. taxpayers to report foreign bank accounts containing amounts over \$10,000, if the taxpayer has a financial interest in, or signature or other authority over, the account. Intentional failure to file subjects the taxpayer to criminal sanctions. Law enforcement agents have conducted a search of the records of Foreign Bank Account Reports database maintained by the Financial Crimes Enforcement Network of the Department of the Treasury (FinCEN) and there is no record of any

FBAR on file for Manafort, [REDACTED] or Gates, during the period 2005 through 2014, for financial accounts located in Cyprus, Latvia, or Grenadines.

13. On April 14, 2017, the Honorable Theresa Carroll Buchanan, pursuant to 26 U.S.C. § 6103, authorized the government to obtain copies of various tax returns for Manafort, Gates, and several of their related business entities. A review of Manafort's personal tax returns shows that in each of tax years 2009 through 2014, he submitted a "Schedule B" form, which provides details regarding the taxpayer's interest and ordinary dividends. The Schedule B form asks, among other things, "At any time during [the tax year in question], did you have an interest in or a signature or other authority over a financial account in a foreign country, such as a bank account, securities account, or other financial account?" In each of tax years 2009 through 2014, Manafort checked the box for "No."

14. A review of Gates's personal income tax returns similarly reveals that in 2010 through 2014, he submitted a Schedule B along with his personal income tax return, and that in each of those years, he indicated that he did not have an interest in or signature or other authority over a financial account in a foreign country.

15. The government's investigation also has developed probable cause to believe that both Manafort and Gates have violated the Foreign Agent Registration Act ("FARA"). FARA provides, as a general matter, that persons acting "at the order, request, or under the direction or control of a foreign principal" and who engages within the United States in political activities in the interests of such foreign principal must register with the Attorney General. 22 U.S.C. § 611. As noted above, Manafort and Gates both acknowledged in interviews with the FBI working on behalf of the Party of Regions, though the work they described supposedly focused on actions overseas.

16. Moreover, the government recently has obtained a large volume of documents from [REDACTED], a political consulting firm based in Washington, DC. The documents are voluminous and have not yet been fully analyzed. Nevertheless, a preliminary review of those documents indicates that [REDACTED] appears to have provided lobbying services on behalf of the European Centre for a Modern Ukraine from approximately 2012 through 2014. The European Centre for a Modern Ukraine is a Pro-Western Ukrainian non-profit group based in Brussels, which acted as an intermediary between the Ukraine and the West to promote Ukraine's political and economic interests. Although the Director of the European Centre for a Modern Ukraine is [REDACTED], emails indicate that Rick Gates acted as an intermediary between the Centre and [REDACTED]

17. A preliminary review of [REDACTED] records reveal, among other things, on February 24, 2012, [REDACTED] sent an email to Rick Gates at [REDACTED] stating:

Thanks so much for meeting with us, for providing us with additional insight on the challenges Ukraine faces and for allowing us the opportunity to share with you the capabilities of our own team. Ukraine certainly faces some challenges in its relationship with the Hill, the administration and the media, especially the NYC and DC press corp. Most notably, the continued imprisonment of Tymoshenko is being utilized by detractors and others who want more diplomatic leverage in their dealings with Ukraine to great success. Yet, this challenge, while formidable, is not insurmountable. An integrated government relations and public relations campaign that includes a strong social media component could go a long way in severing the links between Tymoshenko's political aims and the greater, more important agenda for all Ukraine.

In response, Gates wrote, "I spoke with Paul late last night and told him I thought you and your team did a fantastic job." Based on the context, I believe that the reference to "Paul" in this email is a reference to Paul Manafort.

18. Gates and [REDACTED] also exchanged emails regarding the European Centre for a Modern Ukraine's payments to [REDACTED] [REDACTED] staff would email

work invoices addressed to the European Centre for a Modern Ukraine to Gates. [REDACTED] [REDACTED] was paid more than \$1,000,000 from Cypriot accounts in the name of Bletilla Ventures, from the same account that paid DMP International and Smythson LLC over \$5,000,000, as noted in the chart above. Based upon the email traffic between [REDACTED] and Gates, I believe Gates caused payments to [REDACTED] [REDACTED] from the Bletilla account to satisfy the European Centre for a Modern Ukraine's obligations [REDACTED]

19. As of May 26, 2017, neither Gates nor Manafort had filed a registration statement with the Department of Justice identifying themselves as foreign agents of Yanukovych, the Party of Regions, the European Centre for a Modern Ukraine, or any other Ukrainian-related entity.

20. In addition, law enforcement agents are investigating whether or not all income received by Manafort and Gates was properly reported as required under U.S. law. In the summer of 2016, investigators from Ukraine's National Anti-Corruption Bureau obtained a handwritten ledger said to belong to the Party of Regions ("ledger"). The ledger contains hundreds of pages of entries purporting to show payments made to numerous Ukrainians and other officials

21. The ledger contained entries indicating that Manafort had been paid \$12.7 million by the Party of Regions in 22 separate payments that occurred between 2007 and 2012. U.S. law enforcement is investigating whether any of these sums were paid to Manafort or Gates or others for their benefit.

22. [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] gave him items he said he found in a safe within the office space, including a document purporting to be a contract between Davis Manafort and [REDACTED]

23. The purported contract, dated October 14, 2009, indicates that Davis Manafort promised to sell 501 computers to [REDACTED] for \$750,000.00. The signature page of the contract contains a type-written line indicating that Paul Manafort signed the contract on behalf of Davis Manafort. Above Manafort's type-written name is a signature that purports to be that of Paul Manafort. The point of contact for the buyer, [REDACTED] is listed as [REDACTED] with an address in Belize. The contract identifies two bank accounts for [REDACTED] one in Bishkeyk, Kyrgystan and another in Frankfurt, Germany.

24. The Party of Regions ledger includes an entry dated October 14, 2009, indicating that ██████████ received \$750,000.00. The October 14, 2009, entry also includes a “payment reference” column which states, “Manafort.”

25. Bank records show that on or about October 15, 2009, a \$750,000 payment was wired from an account in Kyrgystan at Asia Universal Bank in the name of [REDACTED] to a Wachovia bank account in Virginia belonging to Manafort.

26. In addition to the October 15, 2009, transaction, bank records show three additional wire transfers totaling \$2,487,500.00 from an account at Asia Universal Bank in the name [REDACTED] to DMP's Wachovia account in the U.S. between June 24 and 25, 2009.

27. When interviewed by law enforcement in 2014, Manafort said he had never heard of a company called [REDACTED]. According to open sources, in response to questions about the ledger, Manafort has said he did not receive any cash for his work in Ukraine.

28. On May 26, 2017, your Affiant met with [REDACTED] a former employee of

Davis Manafort Partners, and a current employee of Steam Mountain, LLC, which is a business currently operated by Paul Manafort. [REDACTED] advised that he is a salaried employee of Manafort's company, and that he performs a variety of functions for Manafort and his companies as directed by Manafort. [REDACTED] advised that, in approximately 2015, at the direction of Manafort, [REDACTED] moved a series of office files of Manafort's business contained in boxes from one smaller storage unit at 370 Holland Lane, Alexandria, Virginia, to a larger storage unit, at the same storage facility, also at 370 Holland Lane, Alexandria, Virginia. [REDACTED] advised that he personally moved the office files into Unit 3013 at that location, and that the files were still in that unit.

29. Later on May 26, 2017, [REDACTED] led your Affiant to the storage facility at 370 Holland Lane, Alexandria, Virginia, where your Affiant obtained a copy of the lease for Unit 3013 from the manager of the storage facility. The lease identifies [REDACTED] as the occupant of Unit 3013, and also identifies Paul Manafort as a person with authorized access to Unit 3013. Richard Gates is listed as an alternate point of contact for the lease.

30. [REDACTED] further provided law enforcement with a key to the lock on Unit 3013 and described the contents of Unit 3013. [REDACTED] advised that Unit 3013 contained several boxes of office files from Manafort's business, as well as a metal filing cabinet containing additional, more recent office files of Manafort's business. [REDACTED] said he moved the filing cabinet from Manafort's former residence in Mount Vernon, Virginia, in the spring of 2015. [REDACTED] indicated that Manafort was using his former residence as an office at the time. [REDACTED] explained that the cabinet was extremely heavy when he moved it, indicating that it contained a large amount of records. Although [REDACTED] could not describe the contents of the filing cabinet in detail, he advised that Manafort occasionally sent emails to [REDACTED] directing [REDACTED] to put certain records

into the filing cabinet on Manafort's behalf. [REDACTED] described the records as "brown, legal-sized files." [REDACTED] recollection is that he last added to the filing cabinet in the spring of 2016.

31. Your Affiant obtained written consent from [REDACTED] to search Unit 3013. [REDACTED] then opened Unit 3013 using the key in his possession in the presence of your Affiant. Without opening any boxes or filing cabinet drawers, I observed inside the unit that there were approximately 21 bankers' boxes that could contain documents, as well as a five-drawer metal filing cabinet. None of the file drawers are marked as to their contents. Some of the boxes are unmarked, while others bear markings. For example, one of the bankers' boxes is marked on the exterior with the following:

Box 2

MPI

- Legal Docs
- Promissory Notes
- Admin
 - o Tax Returns
 - o BOD Resolution
 - o Written Consent of Sole Manager
 - o Seiden COI Waiver
 - o Resignation Letters
 - o Certificate of Liability Insurance
 - o Director's Insurance
 - o Trade Mark
 - o Worker's Comp
 - o MPI Holdings LLC
- Binder contains documents executed in connection with formation and financing of MPI Holdings LLC

32. Another box is marked on the exterior as follows:

Box 5

MPI

- Expenses
- Paid Bills
- Invoices
- Legal Complaints
- Jules Nasso

33. Your Affiant has determined from a search of a public records database that MPI stand for Manhattan Productions International, a film production company, for which Manafort is believed to be an investor. The name suggests that the company has an international scope. Accordingly, it is reasonable that these records may contain evidence of solicitations for and financial transactions involving foreign persons or sources of funds.

34. Another box is marked on the exterior as follows:

Box 12
Ukraine Binders

- Georgia
- Ballot Security
- Surrogates
- Admin
- Research
- RA
- Political
- Polling
- PJM Political Presentation
- Ukraine Campaign
- Media Earned
- Media
- Advance and Training
- Leader

35. For a number of reasons set forth herein it is reasonable to believe that this storage unit is a collection point for Manafort's and Gates's business records from their work in Ukraine. These include that there is a box marked "Ukraine," that [REDACTED] has advised the affiant that he moved business records for Manafort into the storage unit, and because Manafort and Gates—who is listed on the lease as a contact for the lessor—worked together in Ukraine. It is also reasonable to believe that these records and those in the filing cabinet will include financial records for several reasons. These include, but are not limited to, IRS guidelines recommending that persons and corporations generally retain business records for three years from filing of

returns for and seven years if the tax payer had certain losses or bad debts.

36. Your affiant also saw a box marked "movie production stuff," four boxes marked "'96 convention," and three boxes marked "1979 convention," "1988 convention" and "1992 convention, respectively. Because the records go back over 30 years, I believe records relating to Manafort's and Gates's work in Ukraine, including financial records, were retained and may be contained within the storage unit.

37. From my training and experience, I am also aware that individuals and businesses often retain copies of contracts and other business and financial records in anticipation of litigation. Public sources reveal that Manafort was sued by his former client, Oleg Deripaska, sometime in or about 2008. Therefore, it is reasonable to believe historical records have been retained by Manafort and Gates.

38. After I accompanied [REDACTED] to the storage unit described in Attachment A and conducted a review of the contents without opening any box or file drawer on May 26, 2017, the unit was locked with a key. Access to the facility by leaseholders and members of the public was foreclosed by the company from 9:00 pm on May 26, 2017 until approximately 7:00 am on May 27, 2017. Law enforcement agents have surveilled the only entrance and exit to the unit since the time the unit was locked on May 26, 2017 until 9:00 pm, and beginning again at 6:30 am on May 27, 2017, before the business was open to the public or leaseholders. No one has been observed entering or leaving the unit.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

39. In my training and experience, I have learned that U.S. businesses routinely generate and maintain records of correspondence and financial records on computers. For a variety of reasons, copies of historical records and current records are frequently stored on

external hard drives, thumb drives and magnetic disks. There is reasonable cause to believe such media may be contained in and among records of the Mananfort's and Gates's business in the storage unit.

40. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES described in Attachment A, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media.³ Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

41. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

³ A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

42. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the

search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under

investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
 - d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
 - e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
43. *Necessity of seizing or copying entire computers or storage media.* In most cases,

a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or

knowledge will be required to analyze the system and its data on the Premises.

However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

44. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

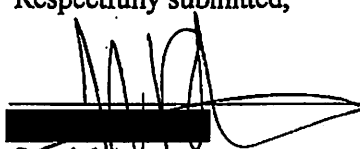
REQUEST FOR SEALING

45. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, and many of the details of the investigation are not yet public. Accordingly, there is good cause to seal these documents because their premature disclosure may give subjects and witnesses an opportunity to move outside of U.S. jurisdiction or to destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation. Similarly, witnesses located abroad may take steps to compromise the investigation.

CONCLUSION


46. Based on the foregoing, I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,


Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on 5/27, 2017

/s/


Theresa Carroll Buchanan
United States Magistrate Judge
THERESA CARROLL BUCHANAN
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is the storage unit located at 370 Holland Lane, Unit 3013, Alexandria, Virginia 22314, as well as any locked drawers, locked containers, safes, computers, electronic devices, and storage media (such as hard disks or other media that can store data), found therein. The storage unit is further described as a metal corrugated steel room with a red and white sign on the exterior with the number 3013.

ATTACHMENT B

Property to be seized

1. Records relating to violations of 31 U.S.C. §§ 5314, 5322(a) (Failure to File a Report of Foreign Bank and Financial Accounts), 22 U.S.C. § 618 (Foreign Agent Registration Act), and 26 U.S.C. § 7206(a) (Filing a False Tax Return), including:

- a. Any and all financial records for Paul Manafort, Richard Gates or companies associated with Paul Manafort or Richard Gates, including but not limited to records relating to any foreign financial accounts;
- b. Any and all federal and state tax documentation, including but not limited to personal and business tax returns and all associated schedules for Paul Manafort, Richard Gates, or companies associated with Paul Manafort or Richard Gates;
- b. Letters, correspondence, emails, or other forms of communications with any foreign financial institution, or any individual acting as the signatory or controlling any foreign bank account;
- c. Any and all correspondence, communication, memorandum, or record of any kind relating to the Party of Regions, Viktor Yanukovich, the European Centre for a Modern Ukraine, or any other foreign principal of Paul Manafort or Richard Gates, or any company associated with Paul Manafort or Richard Gates;
- d. Any and all correspondence, memorandum, press release, or documentation of any kind regarding any lobbying or advocacy performed by Paul Manafort, Richard Gates, or any company associated with Paul Manafort or Richard Gates, on behalf of the Party of Regions, Viktor Yanukovich, the European Centre for a Modern

Ukraine, or any other foreign principal of Paul Manafort, Richard Gates, or any company associated with Paul Manafort or Richard Gates.

- e. Records related to, discussing, or documenting Neocom Systems, Antes Management, Yiakora Ventures, Global Highway Ltd., Global Endeavor, Leviathan Advisors, Peranova Holdings, Bletilla Ventures, Lucicle Consultants, and/or Telmar Investments, including but not limited to bank records, canceled checks, money drafts, letters of credit, cashier's checks, safe deposit records, checkbooks, and check stubs, duplicates and copies of checks, deposit items, savings passbooks, wire transfer records, and similar bank and financial account records.

- f. Records related to, discussing, or documenting [REDACTED]

- g. Any and all daily planners, logs, calendars, schedule books relating to Paul Manafort or Richard Gates.

2. Computers or storage media used as a means to commit the Target Offenses.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web

pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.